Privacy Impact Assessments Overview

Overview

The Defense Health Agency (DHA) is committed to the protection of beneficiary patient and sensitive data. Concurrently, DHA must strive to make it possible to appropriately and lawfully access that information as required to fulfill the Department of Defense (DoD) Military Health System (MHS) mission.

What is a PIA?

A PIA is an analysis of how personally identifiable information (PII) is handled to:

- Ensure data handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the need, privacy risks and effects of collecting, maintaining, using and disseminating PII in electronic form; and
- Examine and evaluate protections and alternative processes to mitigate potential privacy risks.

When is a PIA required?

As stated in DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009, a PIA is required for information systems and electronic collections in the following situations:

> "(1) For existing DoD information systems and electronic collections for which a PIA has not previously been completed, including systems that collect PII about Federal personnel and contractors.
>
> (2) In accordance with Reference (d), for new information systems or electronic collections:
>
> (a) Prior to developing or purchasing new information systems or electronic collections;
> (b) When converting paper-based records to electronic systems; or,
> (c) When functions applied to an existing information collection change anonymous information into PII.
>
> (3) For DoD information systems or electronic collections with a completed PIA, when change creates new privacy risks including the examples stated in subparagraphs 1.b.(3)(a) through 1.b.(3)(f)."

PIAs are applicable to systems that collect, maintain, use, or disseminate PII on beneficiaries or employees. Some examples of PII include:

- Name
- Social Security Number
- Age
- Date and Place of Birth
- Mother's Maiden Name
- Biometric Records
- Marital Status
- Military Rank or Civilian Grade
- Race
- Salary
- Home/Office Phone Numbers
- Other Personal Information which is linked to a Specific Individual

It is important to note that not all examples will be covered in DoD regulations. All the combinations of data elements that can comprise PII are too exhaustive to mention. Consequently, one can combine a seemingly innocuous data element such as number of years of military service with rank and come up with potential PII.

DoDI 5400.16 mandates PIAs be reviewed and updated every three years and/or when there is a significant system change.

Who must fill out a PIA?

OMB M-03-22 guidance applies to all Executive Branch departments and agencies and their contractors that use information technology or that operate
Web sites for the purposes of collecting, maintaining, using or disseminating PII about members of the public, federal personnel, contractors, or in some cases foreign nationals. In addition, relevant cross-agency initiatives, including those to further electronic government are included.

Additional Resources

DHA Privacy Office Web Site - http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties
DoDI 5400.16 - http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf
DD Form 2930 - http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2930.pdf

References

E-Government (E-Gov) Act of 2002, Section 208
DoDI 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, February 12, 2009
DoDI 8500.01, Cybersecurity, March 12, 2014
DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007
DoD 5400.11-R, Department of Defense Privacy Program, May 14, 2007

References (continued)

DoD 6025.18-R, DoD Health Information Privacy Regulation, January 24, 2003
OMB Memorandum 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003
OMB Circular No. A-11, Section 53
OMB Circular No. A-130